UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,817	07/16/2003	Stephen F. Bisbee	003670-104	1237

7590 09/02/2009

Burns, Doane, Swecker & Mathis, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
09/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/620,817	BISBEE ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11 and 15-35* is/are pending in the application.

4a) Of the above claim(s) *19-33* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,15-18,34 and 35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 August 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A response to the notice of non-compliant amendment was received on 10 April 2009. By this response, Claims 1-11, 15-18, 34, and 35 have been amended. Claims 12-14 have been canceled. No new claims have been added. Claims 19-33 were previously withdrawn from further consideration as drawn to a nonelected invention. Claims 1-11, 15-18, 34, and 35 are currently under consideration in the present application.

Response to Arguments

2. Applicant's arguments with respect to claims 1-11, 15-18, 34, and 35 have been considered but are moot in view of the new ground(s) of rejection.

Drawings

3. The objections to the drawings for failure to comply with 37 CFR 1.84(p)(5) are withdrawn in light of the amendments to the drawings and specification.

Specification

4. The objection to the disclosure for informalities is withdrawn in light of the amendments to the specification. Applicant's cooperation is again requested in correcting any other errors of which applicant may become aware in the specification.

5. The objection to the specification for failure to provide proper antecedent basis for the claimed subject matter is withdrawn in light of the amendments to the claims.

Claim Objections

6. The objection to Claims 2, 5, and 18 for informalities is withdrawn in light of the amendments to the claims.

7. Claims 4 and 10 are objected to because of the following informalities:

In Claim 4, in the list in lines 4-7 of the claim, it appears that the comma after "the CA", the comma after "LDAP", and the comma after "time-to-live data element" should be replaced by semicolons, to make clearer the delineation of the items in the list. Additionally, it appears that "and" or "or" should be inserted between "OCSP" and "LDAP".

In Claim 10, line 3, it appears that "are" should be replaced by "is" to agree with the subject "information".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The rejection of Claims 34 and 35 under 35 U.S.C. 112, first paragraph, for failure to comply with the written description requirement is withdrawn in light of the amendments to the claims. The rejection of Claims 5, 9, 11-18, and 34 under 35 U.S.C. 112, second paragraph, as indefinite is NOT withdrawn. Although the issues raised in the previous Office action have been addressed, the amendments to the claims raise further issues of indefiniteness as detailed below.

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1-11, 15-18, 34, and 35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites "the certificates" in lines 6-7. It appears that this may be intended to refer to the "authentication certificates" in line 2; however, it appears that those authentication certificates are not intended to refer to any particular certificates and is just part of the statement of intended use of the method, and therefore the antecedent basis of "the certificates" is not entirely clear. Claim 1 further recites "the CSS's status cache" in line 8; however, there is no clear antecedent basis for this limitation in the claim. The claim further recites "fetching all certificate status reporting methods and communications information from a configuration store of the CSS that are needed for retrieving a status of each certificate whose status has not yet been determined from

the respective issuing CAs" in lines 10-14. First, it is unclear what the phrase "from a configuration store" is intended to modify. Further, it is unclear what the subject of the phrase "that are needed for retrieving" is intended to be; from the placement, it appears that the subject is intended to be "the CSS", however, the verb "are" does not agree with this subject, nor does it appear to clearly make sense. Additionally, it is unclear what the phrase "from the respective issuing CAs" is intended to modify. Claim 1 also recites "processing the certificate statuses according to an appropriate certificate status reporting method" in lines 22-23 of the claim. It appears that, since there may be more than one certificate status, there may also be more than one reporting method to be used, and therefore, "an" appropriate method as recited does not clearly reflect this. The claim further recites "the CSS's cache memory" in line 28; there is insufficient antecedent basis for this limitation in the claim, although it appears that it may be intended to refer to the status cache recited in line 8. Claim 1 additionally recites "wherein the issuing CAs and connector parameters are designated on a list of approved CAs in the configuration store that enable the CSS to interwork with any CAs and CA domains even though they can operate using dissimilar certificate practices and policies" in lines 30-33 of the claim. This is generally unclear. First, it is not clear what the subject of the verb "enable" is intended to be; from the placement of the phrase, it appears that "configuration store" would be the subject, but this does not agree in number with "enable". Further, it is unclear what the antecedent of the pronoun "they" is intended to be. All of the above renders the claim indefinite.

Claim 2 recites "the certificate" in lines 3-4; however, there is more than one certificate recited in Claim 1, and it is not clear to which certificate this is intended to refer.

Claim 3 recites "the organization" in lines 8 and 9; however, the claim earlier refers to "at least one organization" in line 2. Because there can be more than one organization, it is not clear to which of these organizations the limitation "the organization" is intended to refer.

Claim 4 recites "adding at least a status reporting component…" in lines 4-5 of the claim. It is not clear what the component, method, and information are added to.

Claim 5 recites "the certificate status" in line 3 of the claim and "the certificate" in line 5. There is more than one certificate and more than one status recited in the claims, and therefore, it is not clear to which certificate and status these limitations are intended to refer.

Claim 9 recites "the connector" in lines 1-2. However, Claim 1 recites plural connectors in line 16 of the claim, and therefore, it is not clear to which connector this limitation is intended to refer.

Claim 11 recites "the certificate" and "the approved CA" in lines 2 and 3. However, Claim 1 recites plural certificates and plural approved CAs, and it is not clear to which certificate and CA these limitations are intended to refer. Claim 11 further recites a step with the conditional "if the status type is CRL, the CRL in the cache memory is current, and the status is not found in the cache memory" in lines 13-16, and another step with the conditional "if the CRL is not current or found in the cache memory

and local time is greater than a next scheduled publication time for the CRL or the status type is not CRL" in lines 17-21 of the claim. However, it is not clear whether the steps following the second conditional (see lines 22-34) are intended to be performed always or only if the second condition is met. Therefore, it is not clear exactly which steps are to be performed in what situations. The claim additionally recites "the CA" in line 24; again, Claim 1 recites plural CAs, and therefore it is not clear to which CA this limitation is intended to refer.

Claim 15 recites "the threshold" in line 14; however, in line 12, the claim recites plural thresholds, and therefore, it is not clear to which threshold the limitation is intended to refer. Claim 15 also recites "the status" in line 14. Claim 1 recites plural certificates statuses, and it is not clear to which status this limitation is intended to refer.

Claim 16 recites "The CSS of claim 15"; however, Claim 15 has been amended to be directed to a method. Claim 16 further recites "a threshold" in line 5; it is not clear if this is intended to refer to one of the thresholds recited in Claim 15, or to a different threshold.

Similarly to Claim 16, Claim 17 recites "The CSS of claim 16", and Claim 18 recites "The CSS of claim 17". However, Claims 15 and 1, from which these claims ultimately depend, are directed to methods.

Claim 35 recites "that CSS" in lines 2-3; however, the claim recites "any CSS" and also "any other CSS", and it is not clear to which CSS "that CSS" is intended to refer.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1-11, 15, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koehler, US Patent 6301658, in view of Barrett et al, US Patent 6581059.

In reference to Claim 1, Koehler discloses a method of providing a Certificate Status Service ("CSS") for checking validities of authentication certificates issued by respective issuing Certification Authorities ("CAs") that includes receiving certificate status queries from requesting entities (column 5, lines 42-62); if the current statuses are found in the status cache, providing those certificates' statuses (column 6, lines 9-27); if at least one status needs to be determined, fetching information needed for retrieving a status of an authentication certificate from a respective issuing CA (column 5, lines 14-20); configuring connectors based on the identified information for communicating with the issuing CA and communicating with the issuing CA according to the configured connector when the status of the authentication certificate is queried

(column 5, lines 46-55); retrieving the status of the authentication certificate (column 5, lines 53-55; column 6, lines 1-3); processing the certificate statuses according to an appropriate certificate status reporting method that includes CRLs (column 7, lines 12-34); recording retrieved certificate statuses in the cache (column 7, lines 35-58); and returning the retrieved statuses to the requesting entities (column 7, lines 35-58); where the issuing CA and the connector are designated on a list in a configuration store (column 6, lines 3-8). However, Koehler does not explicitly disclose checking a list of approved CAs for the issuing CAs.

Barrett discloses a method in which an issuing CA is checked against a list of approved CAs, and if the CA is not on the list of approved CAs, returning an invalid status for the certificate (column 7, lines 47-63). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Koehler to include a list of approved CAs as disclosed by Barrett, in order to prevent the use of a false CA (see Barrett, column 7, lines 47-51).

In reference to Claim 2, Koehler and Barrett further disclose that certificate is considered to have expired if a local date and time fall outside a validity period indicated in the authentication certificate (Koehler, column 5, line 65-column 6, line 3).

In reference to Claim 3, Koehler and Barrett further disclose that the issuing CA is added to a list of approved CAs by vetting and approving the issuing CA according to predetermined business rules, and if the issuing CA is vetted and not approved, the issuing CA is added to a list of not-approved CAs in the configuration store (Koehler, column 5, lines 21-36; column 8, lines 16-21; Barrett, column 7, lines 47-63).

In reference to Claim 4, Koehler and Barrett further disclose that vetting and approving the issuing CA includes registering a representation of the CA's trusted authentication certificate with the CSS and adding a status reporting component, the status reporting method such as CRL, a time-to-live data element, and configuration information for a connector (Koehler, column 7, lines 12-16; column 8, lines 21-36).

In reference to Claim 5, Koehler and Barrett further disclose checking and updating a local cache memory for certificate status, and if the status is found in the local cache memory and the local date and time are within the certificate's validity period; and if the status is not found in the local cache memory, the CSS establishes a communication session with a certificate status reporting component of the issuing CA, composes a certificate status request according to the configured connector, retrieves the status from the certificate status reporting component, closes the communication session with certificate status reporting component, and adds at least the authentication certificate's identification, status, and time-to-live to the local cache memory (Koehler, column 5, line 65-column 6, line 27).

In reference to Claim 6, Koehler and Barrett further disclose that the certificate status is indicated to be a Certificate Revocation List (CRL), according to a publication schedule of the issuing CA and that the CSS retrieves the CRL from a certificate status reporting component listed in the configuration store, the CSS clears a cache memory associated with the issuing CA, and the CSS determines the status of the authentication certificate from the CRL and stores the status in the cache memory associated with the issuing CA (Koehler, column 5, line 65-column 6, line 27).

In reference to Claim 7, Koehler and Barrett further disclose that when the certificate status is indicated by a Delta Certificate Revocation List ("ΔCRL"); upon notification by the issuing CA that a ΔCRL is available, the CSS retrieves the ΔCRL from a certificate status reporting component listed in the configuration store; if the ΔCRL is a complete CRL, then the CSS clears a cache memory associated with the issuing CA, determines the status from the CRL, and stores the status in the cache memory; and if the ΔCRL contains only changes occurring after publication of a full CRL, the CSS determines the status from the ΔCRL, and stores the status in the cache memory (Koehler, column 7, lines 12-34).

In reference to Claim 8, Koehler and Barrett further disclose communicating according to a sequence of connectors (Koehler, column 5, lines 42-46; column 8, lines 37-45).

In reference to Claim 9, Koehler and Barrett further disclose more than one certificate status checks in a single communicating step (Koehler, column 5, lines 42-46; column 8, lines 37-45).

In reference to Claim 10, Koehler and Barrett further disclose that the certificates are held in the cache until expiration and information is extracted as needed (Koehler, column 5, line 63-column 6, line 8).

In reference to Claim 11, Koehler and Barrett further disclose that retrieving a status of the certificate issued by the approved CA in response to a query from a trusted third-party repository of information objects to the CSS to validate the authentication certificate's status includes locating and reporting the status if the status is present and

current in the cache memory of the CSS (Koehler, column 5, line 63-column 6, line 8); and if the status is not present, performing the steps of: obtaining a status type and retrieval method from a CSS configuration store (Koehler, column 5, line 63-column 6, line 8); if the status type is CRL and the cached CRL is current, but the status is not found in the cache memory, then reporting the status as valid (Koehler, column 6, lines 9-27); if the CRL is not current or not found or the status type is not CRL, then creating a connector and composing a certificate status request according to the status type (Koehler, column 6, lines 9-27, if no entry, status composed from repository); establishing a communication session with a status reporting component of the issuing CA (Koehler, column 5, lines 48-55; column 6, lines 28-41); retrieving the status from a status reporting component of the issuing CA using the obtained retrieval method and ending the communication session (Koehler, column 6, lines 56- 66); interpreting the retrieved status (Koehler, column 6, lines 56-66); associating, with the interpreted retrieved status, a time-to-live value representing a period specified by a CSS policy for the status type (Koehler, column 6, lines 56-66); adding at least one of the certificate's identification, status, and time-to-live values to the cache memory (Koehler, column 5, line 63-column 6, line 8); and reporting the status to the trusted third-party repository of information objects (Koehler, column 8, lines 2-21).

In reference to Claim 15, Koehler and Barrett further disclose reporting valid certificate status when the status type is CRL, the CRL is current, and the status is not cached (Koehler, column 6, lines 9-27); reporting the status when status is found in the cache memory and the time-to-live and use-counter values have not exceeded

thresholds (Koehler, column 7, lines 35-58; column 5, lines 47-49); if the time-to-live or use-counter threshold is exceeded, clearing the status from the cache memory (Koehler, column 5, lines 47-49); if the status has not yet been reported, requesting and retrieving the status using the status type (Koehler, column 7, lines 12-58); when the status type is CRL, retrieving and parsing the new CRL at the next publication (Koehler, column 7, lines 12-34); when the status is a real-time certificate status reporting protocol, retrieving the status (Koehler, column 6, lines 9-27; column 5, lines 53-55); adding at least the certificate's identification, status, and time-to-live data element to the cache memory (Koehler, column 5, line 63-column 6, line 8); and reporting the retrieved status (Koehler, column 5, line 63-column 6, line 8).

In reference to Claim 35, Koehler and Barrett further disclose that any CSS can query any other CSS for the certificate status if that CSS is designated as an approved status reporting component for the CA (see Barrett, column 7, lines 47-63; Koehler, column 5, line 63-column 6, line 8).

13. Claims 16-18 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koehler in view of Barrett as applied to claim 15 above, and further in view of Konheim, US Patent 4264782.

In reference to Claim 16, Koehler and Barrett disclose everything as described above with reference to Claim 15; however, Koehler does not explicitly disclose incrementing or decrementing a status use-counter data element. Konheim discloses a status use-counter data element that is added to the cache memory; is incremented or

decremented every time the certificate's status is checked; and if the status use-counter data element passes a threshold, then the status is reported and .the cache memory is cleared with respect to the status (column 11, lines 58-68; column 12, lines 37-47; see also Koehler, column 7, lines 35-58). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the method of Koehler and Barrett by including a use-counter to check memory access in order to protect against the re-use of a previously verified transaction (Konheim, column 7, lines 4-6).

In reference to Claim 17, Koehler, Barrett, and Konheim further disclose that a status last-accessed data element is added to the cache memory, and the status last-accessed data element in conjunction with the status use-counter data element enable determination of an activity level of the certificate's status (Koehler, column 6, lines 17-22).

In reference to Claim 18, Koehler, Barrett, and Konheim further disclose that when a request is made to the CSS to retrieve a status of a new certificate and the cache memory has reached an allocated buffer size limit, the CSS searches the cache memory for a least-accessed data element indicating an oldest date and clears the respective cache memory entry; and the CSS then retrieves the requested status, places it in the cache memory, and provides the requested status (Koehler, column 6, lines 12-27; column 7, lines 52-57, where the timestamp is updated, which thus clears the memory and enters a new value).

In reference to Claim 34, Koehler, Barrett and Konheim further disclose a cleanup process that removes stale cache entries as required (Koehler, column 6, lines 12-27; column 7, lines 52-57).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kocher, US Patents 6442689 and 7526644, disclose a method in which revocations from many CAs are combined into a single trusted source for revocation.

b. Sussman, US Patent 6836765, discloses a system in which a client keeps a list of trusted CAs.

c. Kwan, US Patent 6970862, discloses a method for answering OCSP requests without necessarily using CRLs.

d. Herzberg et al, US Patent 7024691, discloses a system in which a user includes a list of authorized CAs.

e. Remer et al, US Patent 7076653, discloses a system in which a trusted party includes a list of trusted CAs.

f. Freed et al, US Patent 7149892, discloses a system in which a certificate issuer is checked against a list of trusted CAs.

g. Delany et al, US Patent 7475151, discloses a system in which real time status for a certificate is checked, for example using OCSP.

h. Micali, US Patent 7529928, discloses a system for certificate revocation.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Examiner, Art Unit 2437